Clase 4 — 13.11.25

#ciscopackettracer #network

👨‍🏫 Profesor: Carlos Quintana
📘 Unidad: Ciberseguridad
🗓️ Clase 3— 13/11/2025
🎯 Tema: unir dos redes independientes con AAA + IoT mediante enrutamiento, simulando dos viviendas o sedes diferentes.

1️⃣8️⃣ Extensión del escenario: dos viviendas inteligentes que deben comunicarse

El profesor plantea una situación más realista: **dos redes IoT totalmente separadas**, cada una con su propio servidor AAA-DHCP, con sus dispositivos inteligentes, con sus usuarios y con su propio punto de acceso inalámbrico. El objetivo es lograr que:

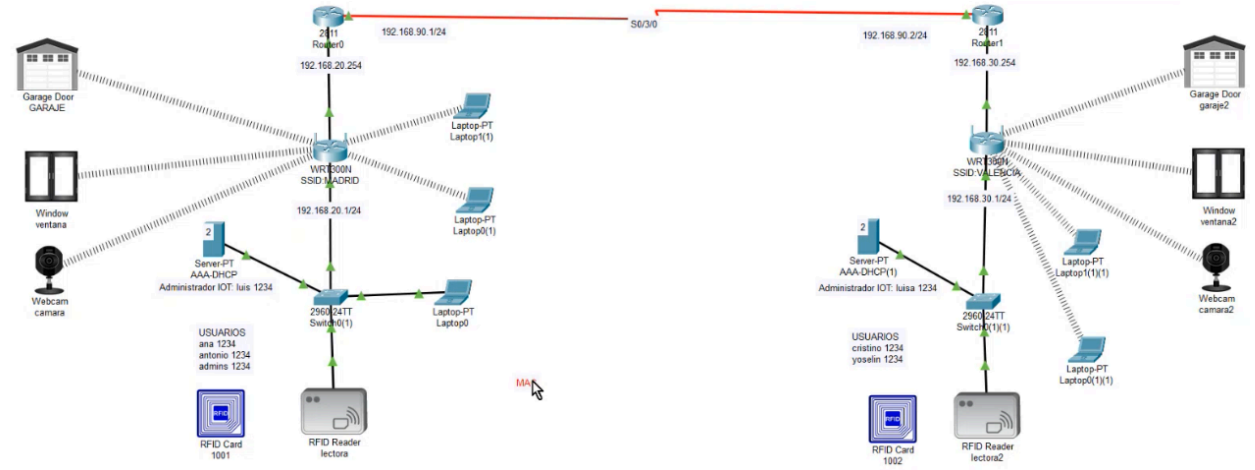
- los dispositivos IoT de un lado puedan ser gestionados desde el otro,
- los dos servidores AAA puedan verse mutuamente,
- las dos redes se comuniquen sin mezclar sus segmentaciones internas,
- todo ello manteniendo una arquitectura segura basada en AAA, DHCP centralizado y autenticación individual.

Este escenario es común cuando una empresa tiene **dos sedes** (por ejemplo, Madrid y Valencia) y quiere que, pese a ser redes independientes, exista **interconexión segura** para gestión y soporte. También es aplicable en smart homes: una vivienda principal y una segunda residencia que comparten infraestructura de control.

El profesor utiliza Packet Tracer para representar esta situación.

🔧 El punto de partida: dos sistemas totalmente separados

Las imágenes muestran claramente ambos entornos: izquierda y derecha.



Cada “hogar” tiene:

- un servidor AAA-DHCP con IoT Server activado,
- un router doméstico WRT300N actuando como Access Point,

- un switch 2960,
- dispositivos IoT vinculados (puertas, ventanas, cámara, garaje),
- una tarjeta RFID y su lectora,
- usuarios locales y administrador IoT.

Hasta ahora, ambos mundos estaban **incomunicados**, porque cada router hacía de frontera sin nada más allá.

🛑 ¿Por qué NO podemos enrutar directamente los routers domésticos WRT300N?

Es importante entender el porqué:

Los routers domésticos como el WRT300N **no están diseñados para funcionar como routers de backbone**. Son dispositivos pensados para:

- dar WiFi,
- actuar como puerta de enlace local,
- entregar DHCP (si se usa),
- crear una red doméstica pequeña.

Pero **no permiten configuraciones de enrutamiento avanzado**, como:

- rutas estáticas,
- enlaces seriales,
- backbones públicos simulados,
- protocolos profesionales de enrutamiento.

No es que "no quieran": es que **no tienen la capacidad técnica**. Por eso, para interconectar redes LAN separadas, se necesitan routers profesionales como la serie **Cisco 2811**, que sí permiten:

- añadir módulos WIC-2T,
- crear enlaces seriales,
- configurar rutas estáticas o dinámicas,
- actuar como routers WAN reales.

Por eso el profesor introduce **dos routers 2811**, uno en cada extremo.

1️⃣9️⃣ Añadiendo routers 2811 para simular la “red pública”

El profesor apaga el router 2811, abre la vista **Physical**, y le instala un módulo **WIC-2T**, que aporta interfaces seriales para simular conexiones WAN o públicas.

Este paso se repite en ambos lados.

2️⃣0️⃣ Conexión del router 2811 con la red privada de cada lado (explicación ampliada)

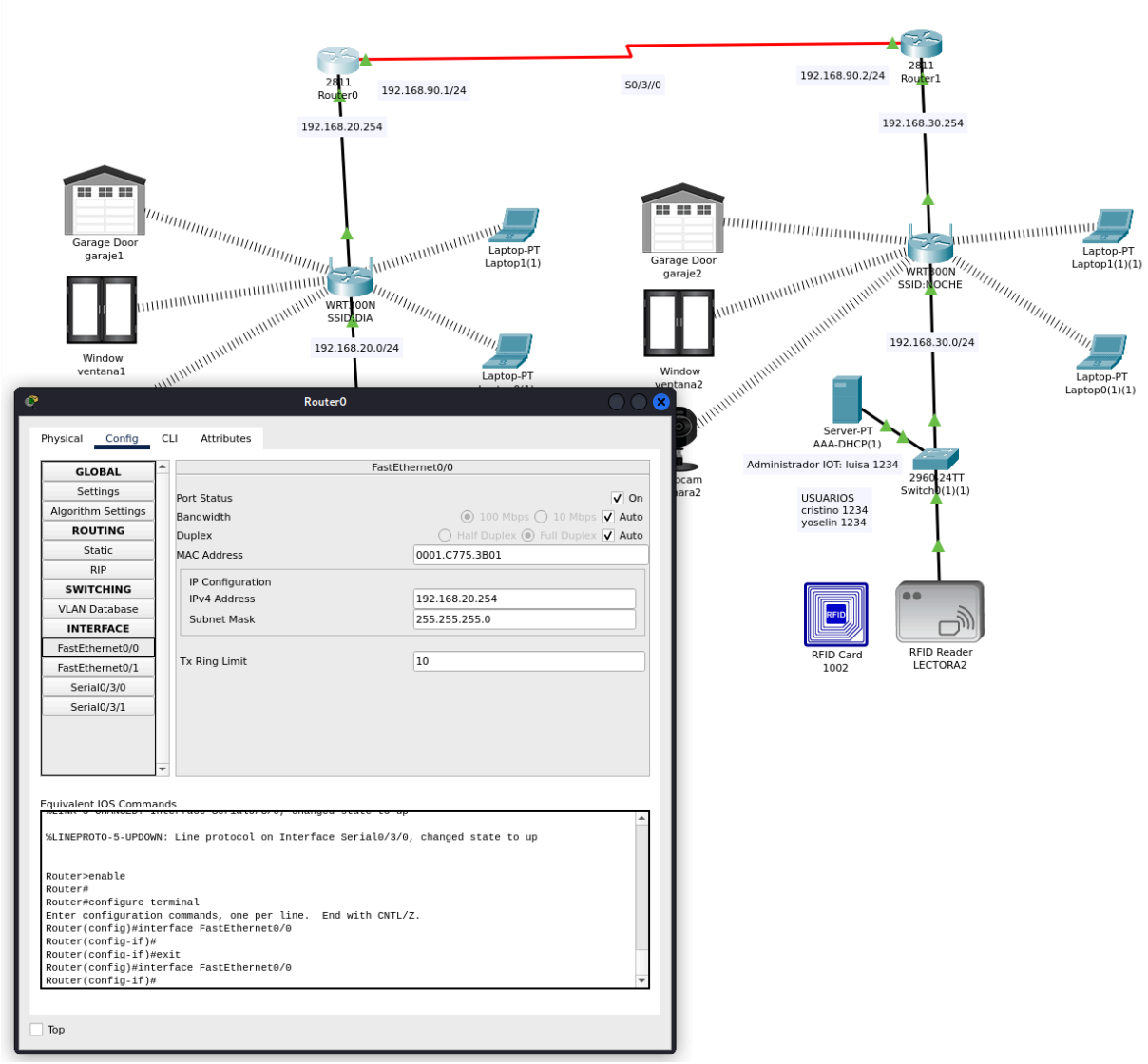
Una vez instalados los módulos WIC-2T en los routers 2811 y preparados los enlaces seriales que más tarde simularán la “red pública”, el profesor explica que el siguiente paso es **integrar cada router profesional dentro de la LAN privada a la que pertenece**. Esto es crucial porque un router no puede enrutar aquello que no conoce; necesita tener un pie en cada territorio que debe interconectar.

En otras palabras:

- el router debe ver “hacia adentro” (LAN doméstica → IoT, WiFi, servidores AAA),
- y debe ver “hacia afuera” (WAN pública simulada → otros sistemas remotos).

El tráfico cruzará siempre por el router si la topología está bien diseñada.

Por ese motivo, cada 2811 se conecta mediante **FastEthernet0/0** directamente al switch de su red local, tal como se ve en la imagen siguiente:



En esta captura puede verse claramente:

- El **Router0 (2811)** está conectado por FastEthernet0/0 al **Switch0** del entorno MADRID.
- El **Router1 (2811)** hace lo propio con el Switch del entorno NOCHE (o VALENCIA).

¿Por qué FastEthernet0/0 y no otro puerto?

Porque:

- Los routers Cisco normalmente usan las interfaces FastEthernet/GigabitEthernet para entrar a LANs locales.
- Los puertos seriales (S0/3/0 o S0/3/1) se usan exclusivamente para enlaces WAN simulados.
- La conexión LAN debe ser rápida, directa y sin complicación física.

Así, FastEthernet0/0 se convierte en la “puerta de entrada” del router hacia su propia red local.

Asignación de la IP “LAN-side” del router 2811

Una vez conectado físicamente, el router debe recibir una **dirección IP perteneciente a la red local en la que está conectado**. En nuestro caso:

En la red de la izquierda (MADRID)

La red LAN es:

```
192.168.20.0/24
```

Por tanto, el router debe tener una IP dentro de ese rango, pero una IP que no esté ocupada por nadie crítico (servidor, AP, etc.). El profesor asigna:

```
Router0 FastEthernet0/0 → 192.168.20.254
```

¿Por qué .254?
Porque es habitual utilizar `.1` para puntos de acceso o switches, `.2` para servidores, y `.254` como **puerta de enlace LAN**. Esto evita conflictos y ayuda a que la topología sea fácil de leer.

La configuración aparece exactamente así en Packet Tracer:

La máscara **255.255.255.0** confirma que el router se encuadra correctamente dentro del /24.

¿Qué implica conectar el router así?

Esta acción convierte al router 2811 en la nueva **puerta de salida** hacia el exterior para toda la red local.

Por eso, en el paso siguiente (punto 21), tuvimos que modificar el **Default Gateway** del servidor AAA de 192.168.20.1 → 192.168.20.254.

El router doméstico WRT300N desaparece de la ecuación WAN:

> pasa a ser únicamente un punto de acceso WiFi, sin capacidad de enrutar tráfico hacia otras redes externas.

Este cambio es intencionado y refleja una arquitectura típica profesional:

- **WRT300N** → solo WiFi (capa de acceso)
- **Switch 2960** → distribución interna
- **Servidor AAA/DHCP/IoT** → control
- **Router 2811** → salida WAN real (interredes)

¿Y por qué necesitamos esto?

Porque queremos unir **dos redes diferentes**, no solo dos WiFis dentro de la misma casa.
Necesitamos una entidad capaz de:

- hablar con redes externas,
- configurar rutas estáticas,
- gestionar enlaces WAN,
- y tomar decisiones de enrutamiento.

El WRT300N **no sirve para eso**:
no soporta rutas estáticas ni módulos WAN profesionales.

Usando FastEthernet0/0 como interfaz LAN

La interfaz FastEthernet0/0 es ideal porque:

- opera a 100 Mbps (suficiente para simular tráfico interno),
- ofrece compatibilidad con cualquier switch Cisco,
- permite direccionamiento IP estándar,
- es fácil de identificar y documentar.

Una vez configurada la IP, el router **ya forma parte de la LAN** y puede:

- recibir paquetes desde los IoT,
- comunicarse con el servidor AAA,
- aparecer en su tabla ARP,
- y servir como gateway.

Este paso es fundamental: **sin esta integración LAN, el router jamás podría enrutar tráfico entre las dos viviendas**.

2️⃣1️⃣ El nuevo Default Gateway de cada servidor AAA

El momento en que introducimos los routers Cisco 2811 supone un cambio conceptual importante en la arquitectura de la red. Hasta este punto, cada “casa” funcionaba como una red autosuficiente donde el servidor AAA-DHCP enviaba su tráfico hacia fuera a través del router doméstico WRT300N. El WRT300N, aunque limitado, actuaba como puerta de enlace porque no existía ningún dispositivo más allá de él.

Sin embargo, en cuanto añadimos los routers profesionales 2811, la estructura se reorganiza siguiendo el modelo real de una red corporativa:

- **el router doméstico deja de ser la puerta de salida**,
- **y el router profesional 2811 pasa a asumir ese rol**,
- ofreciendo un camino lógico hacia otras redes externas.

Esto significa que todas las máquinas internas —servidor AAA, IoT, laptops, actuadores— deben enviar cualquier tráfico “no local” al **Router 2811**, no al WRT300N.

En redes reales, este paso es equivalente a decirle a un servidor:

> “Si quieres hablar con redes que no son la tuya, ve por el router que está preparado para ello”.

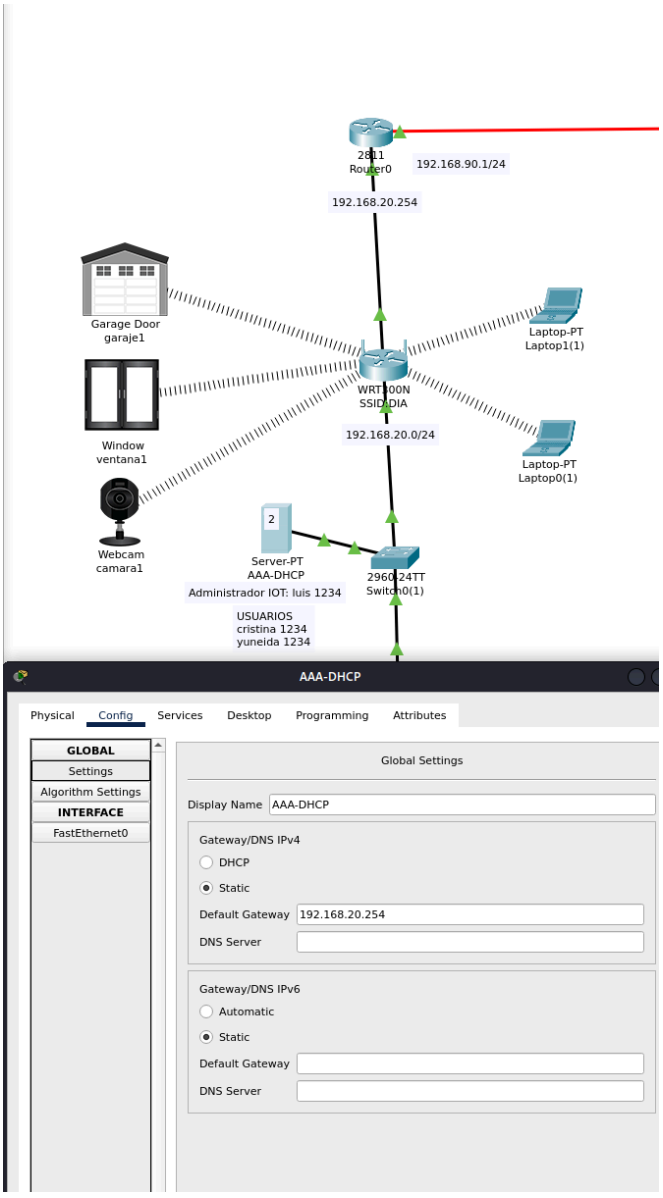
Por eso se cambia el Default Gateway de cada servidor AAA:

🔹 En la red de la izquierda (MADRID)

El servidor usa ahora como salida:

```
Default Gateway = 192.168.20.254
```

Esta IP corresponde a FastEthernet0/0 del Router0 (2811).

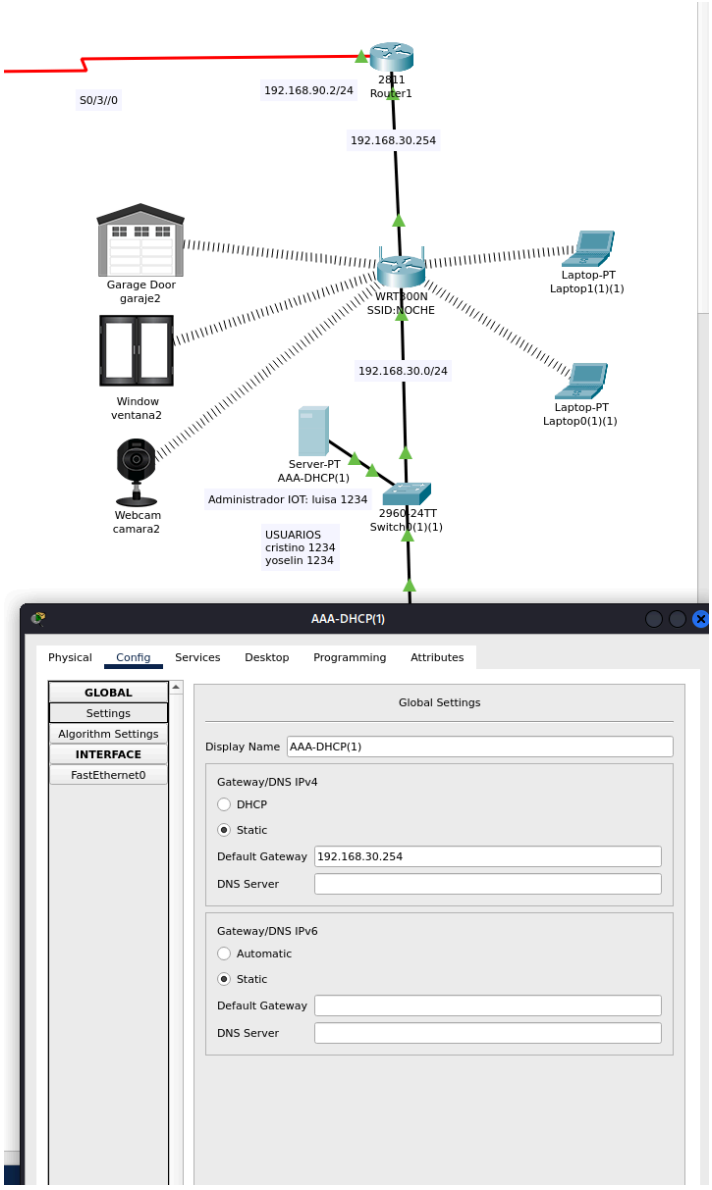


🔹 En la red de la derecha (NOCHE / VALENCIA)

El servidor utiliza:

```
Default Gateway = 192.168.30.254
```

Esta IP es la FastEthernet0/0 del Router1 (2811).



📌 Razón técnica del cambio

Un servidor solo puede comunicarse con redes externas (otras LAN, otras sedes, redes públicas, etc.) si envía sus paquetes a la interfaz correcta. Antes, el único “camino hacia fuera” disponible era el WRT300N, que no tenía capacidad de enrutamiento avanzado.

Ahora, el router 2811:

- conoce rutas hacia otras redes,
- puede gestionar enlaces WAN (serial),
- puede utilizar rutas estáticas (o dinámicas),
- puede manejar múltiples interfaces de red.

En consecuencia, el servidor debe actualizar su Default Gateway para que toda su comunicación externa sea gestionada por el router capaz de enrutar.

Sin este cambio, el servidor no sabría cómo llegar a 192.168.90.0/24 o a 192.168.30.0/24 y se quedaría aislado dentro de su LAN.

💡 Idea clave

Cambiar el Default Gateway no es solo un ajuste de IP:
es declarar explícitamente cuál es el punto de salida válido de una red.

Y en este sistema, **la salida válida y segura es el 2811, no el WRT300N**.

2️⃣2️⃣ Configuración del router izquierdo (Router0 – 2811)

(explicación ampliada y narrada)

Una vez que el servidor AAA ha sido “reorientado” hacia su nuevo gateway, toca configurar las interfaces del router 2811 para que este pueda participar en ambas redes:

- La **LAN interna** (192.168.20.0/24), donde viven el servidor, los IoT y el Access Point.
- La **WAN simulada** (192.168.90.0/24), que conectará esta vivienda con la del otro lado.

La imagen muestra la interfaz FastEthernet0/0 del Router0 ya configurada como puerta de enlace.

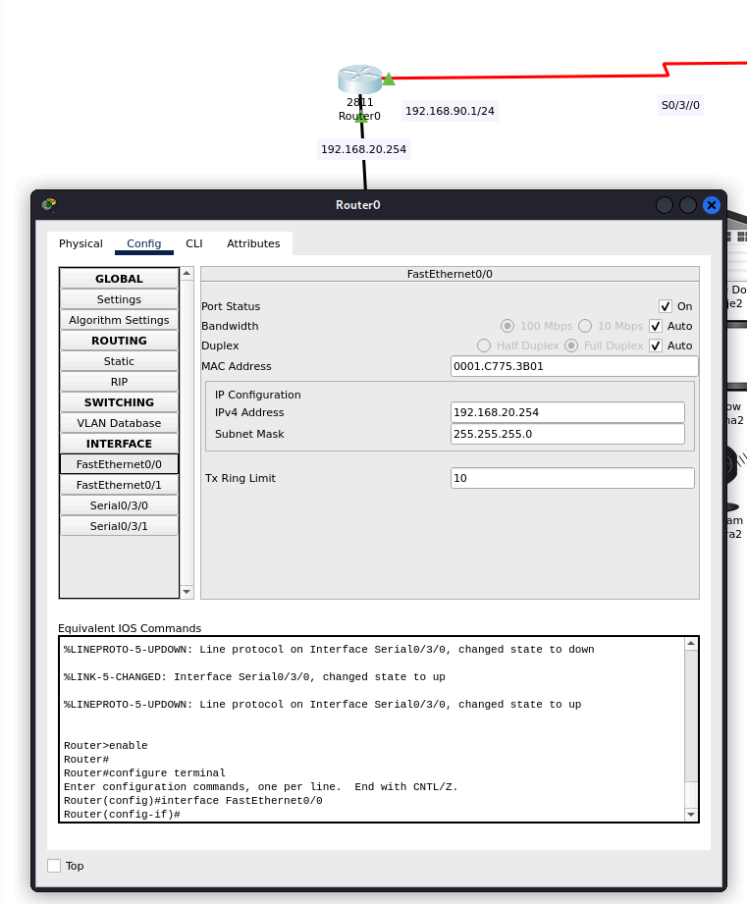
🔹 Configuración de FastEthernet0/0 (lado LAN)

Dentro del menú:

`Config → Interface → FastEthernet0/0`

El profesor asigna:

- **IP:** `192.168.20.254`
- **Máscara:** `255.255.255.0`



Esta interfaz es la que conecta el Router0 al Switch del entorno MADRID.
Gracias a esta IP, el router:

- se convierte en la puerta de enlace oficial de la LAN,

- puede recibir tráfico del servidor y de todos los dispositivos,
- y puede decidir si el tráfico debe permanecer en la LAN o salir hacia la WAN.

Este rol es exactamente el que cumple un router profesional en redes reales:
interconectar dominios de red distintos.

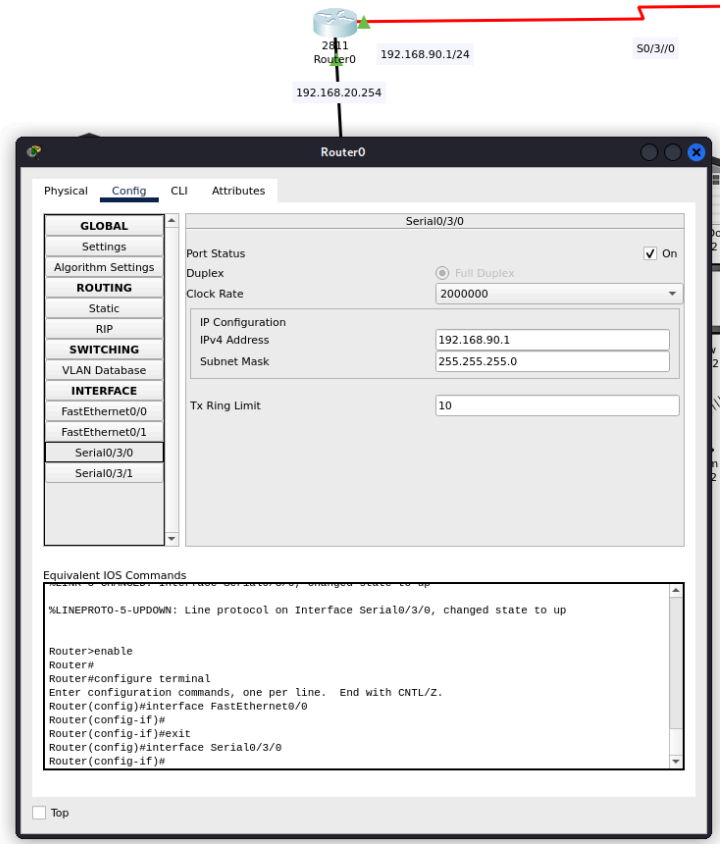
🔹 Configuración de Serial0/3/0 (lado WAN simulada)

Una vez configurada la parte LAN, el profesor pasa a la interfaz serial:

`Config → Interface → Serial0/3/0`

Se asignan:

- **IP:** `192.168.90.1`
- **Máscara:** `255.255.255.0`



Esta interfaz conecta Router0 con Router1 mediante un cable serial DCE/DTE.
El rango 192.168.90.0/24 funciona como una red “pública simulada” o backbone, equivalente a lo que sería un ISP interconectando dos sedes.

En redes reales este enlace sería:

- fibra dedicada,
- un MPLS,
- una VPN de sitio a sitio,
- o una línea arrendada empresarial.

Aquí es solo un cable serial, pero conceptualmente hace lo mismo.

🔹 Importancia de este paso

Con esta configuración, el Router0 ya tiene:

- una **puerta hacia dentro** (FastEthernet0/0),
- una **puerta hacia fuera** (Serial0/3/0),
- una IP válida en cada dominio,
- capacidad para enrutar tráfico entre ambas redes.

En este punto, el router sabe "dónde está" y "qué redes tiene conectadas", pero aún no sabe cómo llegar a la red de la otra vivienda. Ese conocimiento llegará en el punto 2️⃣4️⃣, cuando se añadan las **rutas estáticas**.

🔹 Idea clave

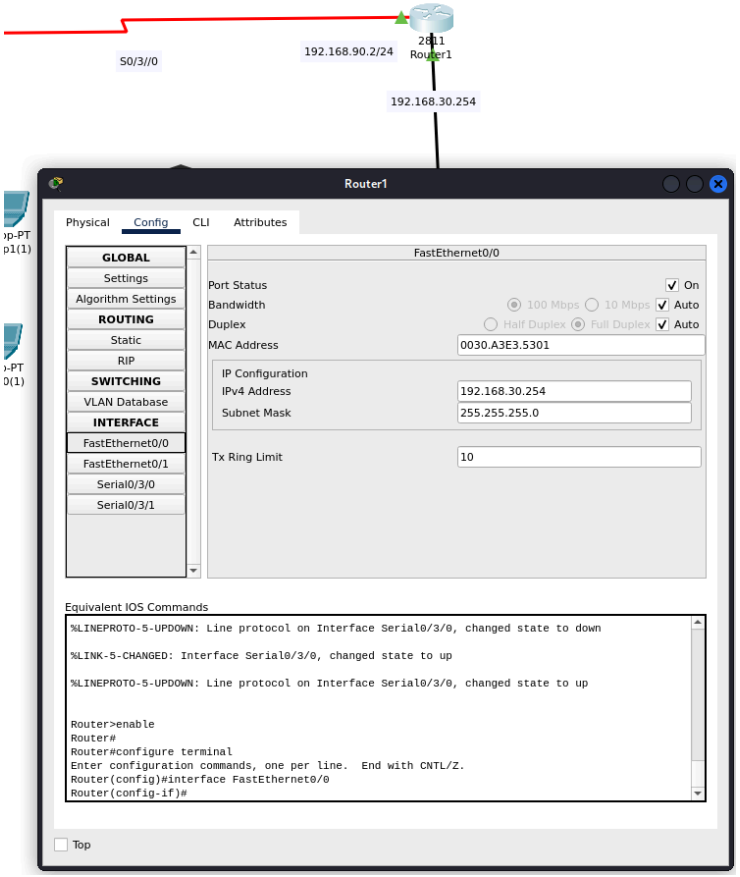
El Router0 2811 no solo divide las redes, sino que **las une** de manera controlada.
Le da estructura a la topología, separa dominios de broadcast y establece el camino de intercomunicación entre sedes que, antes de instalarse, estaban completamente aisladas.

2️⃣3️⃣ Configuración del router derecho (Router1 – 2811)

Una vez configurado el Router0 del lado izquierdo, el profesor procede con la configuración equivalente en **Router1**, situado en la vivienda o sede del lado derecho. La lógica es exactamente la misma, pero aplicada a una red con un rango distinto.

Aquí es importante entender que cada router debe participar en dos redes diferentes:

- **Una red LAN propia**, con sus IoT, su servidor AAA y su switch.
- **Una red WAN común**, usada para conectar las dos sedes.



🔹 Configuración de FastEthernet0/0 — interfaz hacia la LAN derecha

La red local de esta vivienda es:

```
192.168.30.0/24
```

Para integrarse correctamente, el router debe tener una IP dentro de esta red.
El profesor asigna:

```
FastEthernet0/0 → 192.168.30.254  /24
```

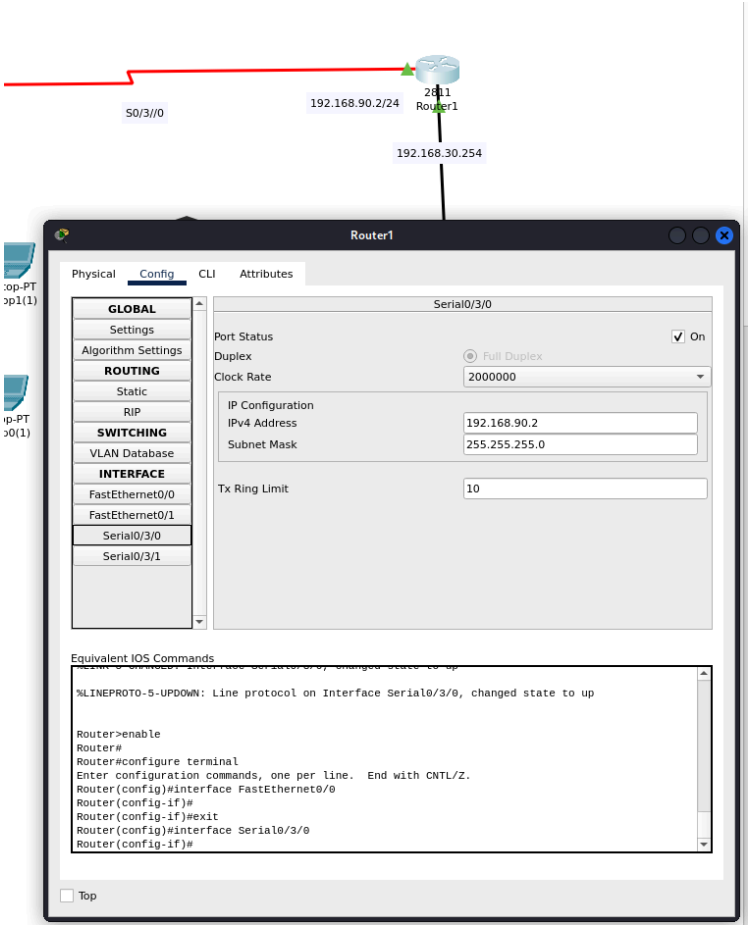
Esta dirección actúa como:

- nueva **puerta de enlace**,
- punto de tránsito hacia otros dominios,
- y enlace entre la red doméstica y la WAN simulada.

Exactamente igual que sucedía en la red de la izquierda, el router profesional reemplaza al WRT300N como gateway, dejando al WRT300N limitado exclusivamente al rol de **Access Point inalámbrico**.

🔹 Configuración de Serial0/3/0 — interfaz hacia la WAN simulada

La interfaz serial de Router1 conecta directamente con el Router0 mediante un cable serial DCE/DTE. Esto simula una línea arrendada, un enlace MPLS o cualquier tipo de conexión WAN empresarial.



El profesor asigna:

```
Serial0/3/0 → 192.168.90.2  /24
```

Esta IP corresponde a la mitad derecha de la red WAN:

```
WAN simulada → 192.168.90.0/24
Router0 → .1
Router1 → .2
```

De este modo, la columna vertebral WAN queda establecida y ambos routers tienen ya una “carretera común” para enviar tráfico entre sí.

📌 ¿Por qué esta estructura es importante?

Porque un router **sin dos interfaces activas en redes diferentes no puede enrutar nada**.
Para enrutar, necesita:

1. **una red de origen**,
2. **una red de destino**,
3. **un camino entre ambas**.

Router1 ya forma parte:

- de la LAN derecha (192.168.30.0),
- y de la WAN central (192.168.90.0).

Ahora le falta aprender **cómo llegar a la LAN izquierda**.
Eso llegará en el punto 2️⃣4️⃣.

2️⃣4️⃣ Enrutamiento estático entre ambas viviendas

(explicación ampliada y narrada)

Una vez que ambos routers están correctamente conectados a sus LAN y a la WAN simulada, llega la parte que realmente “une los mundos”: **crear rutas estáticas**.

Una ruta estática es una instrucción manual del estilo:

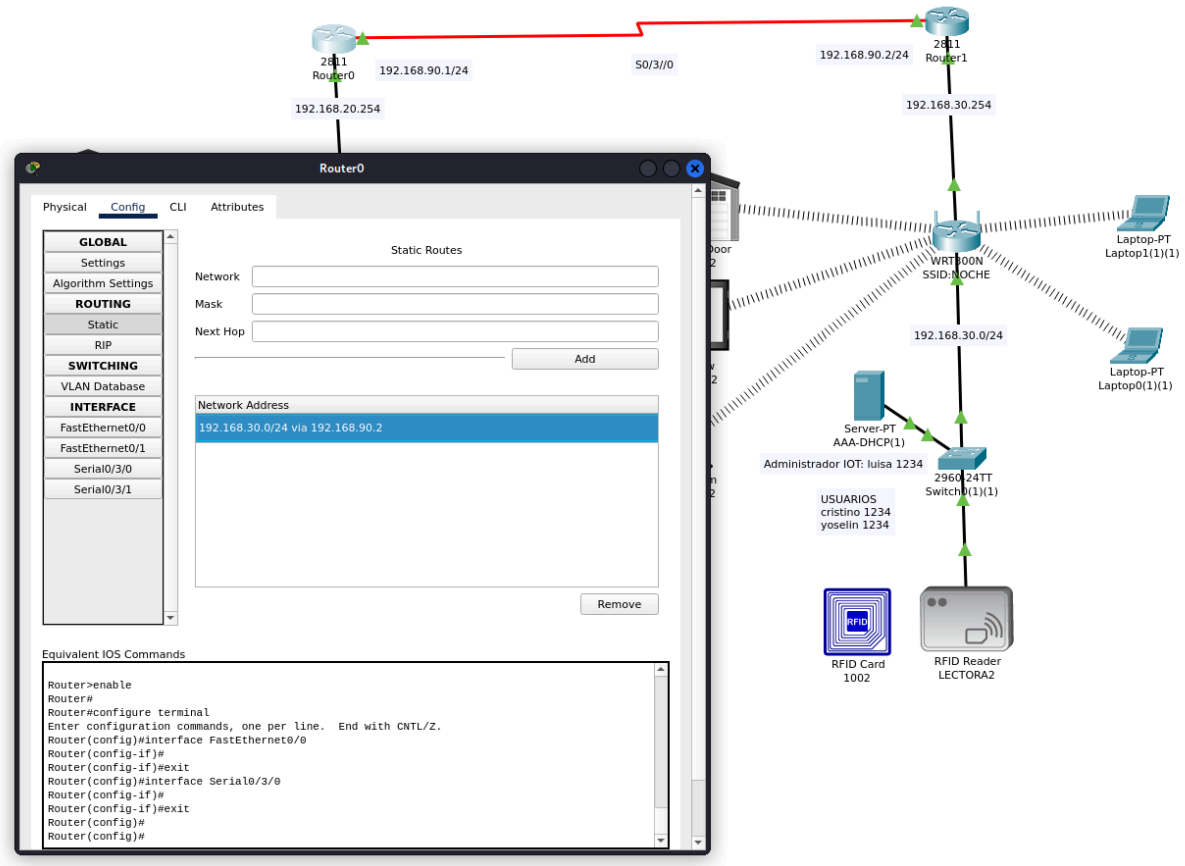
> “Para llegar a esta red, envía los paquetes a este router”.

En topologías pequeñas es habitual usar rutas estáticas por su simplicidad; en redes empresariales más grandes se usan protocolos dinámicos (OSPF, EIGRP, BGP), pero para un ejercicio académico es mejor ver explícitamente cómo funciona la lógica del enrutamiento.

🔹 En Router0 (izquierda)

Router0 conoce:

- la LAN 192.168.20.0/24 (por FastEthernet0/0),
- la WAN 192.168.90.0/24 (por Serial0/3/0).



Pero **no sabe cómo llegar a**:

```
192.168.30.0/24
```

Por ello, el profesor añade una ruta:

```
Network: 192.168.30.0
Mask: 255.255.255.0
Next Hop: 192.168.90.2
```

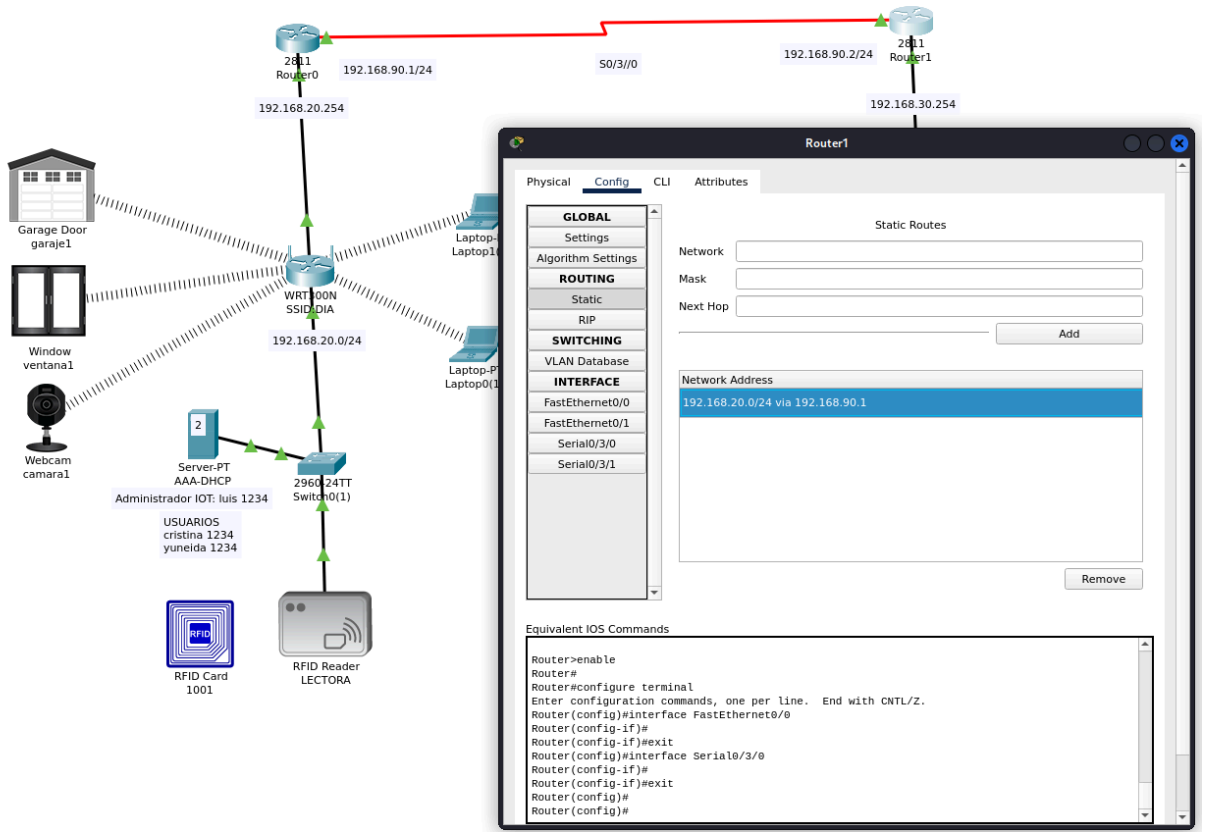
Esta instrucción significa:

> “Para llegar a la LAN derecha, envía el tráfico al Router1 usando su IP WAN”.

🔹 En Router1 (derecha)

Router1 conoce:

- la LAN 192.168.30.0/24,
- la WAN 192.168.90.0/24.



Pero no sabe cómo llegar a:

```
192.168.20.0/24
```

Por eso se añade:

```
Network: 192.168.20.0
Mask: 255.255.255.0
Next Hop: 192.168.90.1
```

Que se interpreta como:

> “Si alguien te pide dirigirte a la LAN izquierda, envía los paquetes al Router0”.

🔹 Resultado final

Con ambas rutas configuradas:

- Router0 puede llegar a la LAN derecha,
- Router1 puede llegar a la LAN izquierda,
- y ambos usan la red 192.168.90.0/24 como **columna vertebral**.

Esto completa la interconexión entre ambos mundos y convierte el conjunto en una red distribuida realista.

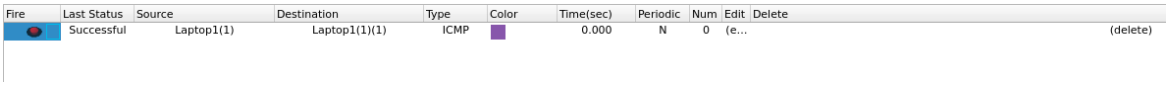
2️⃣5️⃣ Prueba de conectividad

El profesor valida la configuración de la forma más directa: haciendo **ping** entre los dos servidores AAA.

- Servidor de la izquierda → 192.168.20.2

- Servidor de la derecha → 192.168.30.2

El ping es exitoso, lo que confirma:



- que los gateways están bien configurados,
- que los routers enrutan correctamente,
- que las rutas estáticas funcionan,
- que no hay errores de máscara, interfaz o cableado,
- que la red WAN está operativa.

Pero el profesor no se queda ahí. Para demostrar que la infraestructura AAA + IoT funciona de manera distribuida, accede desde el **IoT Mobile** del servidor de la izquierda para iniciar sesión en el servidor derecho usando el usuario:

```
luisa / 1234
```

Y efectivamente:

- aparecen los dispositivos IoT de la red del otro lado,
- las credenciales funcionan,
- las reglas de IoT pueden aplicarse entre redes distintas.

Esto transforma ambas viviendas en un **ecosistema IoT unificado** distribuido en dos sedes.

2️⃣6️⃣ Reflexión del profesor: seguridad, auditoría y accesos fraudulentos

Con la infraestructura ya operativa, el profesor aprovecha para abordar uno de los temas más olvidados en domótica moderna: **la auditoría y el seguimiento de accesos**.

Muchos sistemas comerciales de “smart home” no registran adecuadamente:

- quién abre una puerta,
- quién activa un sensor,
- qué usuario usa una tarjeta RFID,
- desde qué red o dispositivo se produce el acceso.

Esta falta de trazabilidad es peligrosa, porque permite que:

- un instalador deshonesto pueda acceder sin dejar rastro,
- un técnico de mantenimiento pueda abusar de sus permisos,
- un atacante con lector RFID pueda clonar tarjetas,
- un ex-empleado de una empresa de seguridad pueda manipular accesos.

Con un sistema AAA:

- cada acción queda asociada a un usuario concreto,
- hay logs y evidencias de auditoría,
- pueden generarse eventos en tiempo real (correo, syslog, alertas),
- se pueden aplicar roles diferentes (administrador, usuario normal, IoT manager).

Este enfoque es mucho más profesional y evita abusos.

El profesor recomienda, como medida adicional, instalar **una cámara independiente**, aislada de la empresa instaladora y alimentada por energía solar, para tener un registro visual ajeno al ecosistema central. Esto sirve como doble control ante intentos de manipulación o accesos sospechosos.

En entornos domésticos, esta práctica es especialmente valiosa cuando los sistemas están integrados con cerraduras inteligentes, sensores de movimiento y control remoto de accesos.

2️⃣7️⃣ Seguridad física en switches: ataque de intruso por cableado

(explicación ampliada y narrada)

En esta parte de la clase, el profesor introduce un tipo de ataque que muchas veces se pasa por alto en la enseñanza de redes: **los ataques físicos**.
Estamos tan acostumbrados a pensar en firewalls, contraseñas, WPA2, cifrado y servidores AAA que olvidamos la realidad más simple:
si alguien consigue conectar un portátil a tu switch… ya está *dentro* de tu red.

Para demostrarlo, el profesor realiza el experimento más clásico:

> Un intruso se acerca al switch, desconecta el cable del servidor y enchufa en ese mismo puerto su propio portátil.

A nivel eléctrico, el switch no sabe quién ha hecho el cambio. Solo detecta que en ese puerto ahora aparece **una MAC diferente**. Y aquí entra en juego la seguridad del switch:

🔹 Cuando NO hay seguridad configurada en el switch

Si los puertos del switch están abiertos, sin ningún tipo de restricción:

- el portátil del atacante recibe una IP (si hay DHCP),
- entra en la LAN como si fuera un dispositivo legítimo,
- puede intentar acceder al servidor IoT,
- puede intentar utilizar credenciales por fuerza bruta,
- puede explorar la red interna con herramientas como Nmap.

Este es el típico ataque interno que ocurre en oficinas, naves industriales, colegios, hoteles o incluso comunidades de vecinos: basta con llegar al rack o a un punto de red medianamente accesible.

🔹 Cuando el switch SÍ tiene seguridad (port-security)

Si configuramos **port-security**, el panorama cambia radicalmente:

El switch es capaz de:

- **memorizar qué MAC está autorizada en cada puerto**,
- **bloquear automáticamente el puerto** si detecta un dispositivo no autorizado,
- **enviar logs al servidor de monitorización**,
- **bloquear temporal o permanentemente el acceso** (según la política).

En ese caso, al intruso conectar su portátil ocurrirá:

- el switch detecta una **MAC desconocida**,
- identifica el cambio como **movimiento sospechoso**,
- y **bloquea el puerto** inmediatamente.

En redes reales esto se conoce como *MAC violation*.

🔹 ¿Por qué es tan importante la seguridad física?

Las empresas suelen tener una falsa sensación de seguridad basada únicamente en configuraciones lógicas, olvidando que:

- puertos Ethernet son accesibles en escritorios, pasillos, salas de reuniones, etc.,
- un atacante interno o visitante puede aprovechar segundos de despiste,
- muchos ataques comienzan con acceso físico no supervisado.

Por esta razón, las organizaciones deben:

- registrar y limitar MACs conocidas,
- controlar quién tiene acceso a los switches,
- cerrar los armarios de comunicaciones,
- y, como dijo el profesor, instalar **cámaras discretas**, a veces incluso sin señalización visible, que graben cualquier manipulación del cableado.

📌 Ideas clave del profesor

- **La seguridad física es inseparable de la seguridad lógica.**
- Si un atacante obtiene acceso a un puerto abierto, puede saltarse la seguridad WiFi, AAA y firewall de un plumazo.
- El registro y control de MACs es fundamental en redes cableadas.
- Los switches de gama empresarial permiten medidas que los domésticos no tienen.

Este tipo de amenazas ocurre en empresas reales y es una de las razones por las cuales el control de accesos físicos forma parte de cualquier certificación de ciberseguridad (ISO 27001, ENS, PCI-DSS, etc.).

2️⃣8️⃣ Nota final del profesor: aislamiento seguro mediante máquina virtual

Como cierre de la clase, el profesor introduce una idea que traslada la seguridad al ámbito doméstico: el uso de **máquinas virtuales** para navegar por Internet o realizar tareas sensibles.

Explica que una de las formas más efectivas de proteger un ordenador personal es ejecutar el sistema operativo que se conecta al router dentro de una **máquina virtual (VM)**, cargada desde una ISO limpia en programas como:

- VirtualBox,
- VMware Workstation,
- o incluso QEMU/KVM en Linux.

Esto crea una capa de aislamiento muy fuerte:

🔹 Beneficio 1: Aislamiento operacional

El sistema real del usuario queda completamente separado del entorno de navegación.
Si ocurre un ataque (malware, phishing, troyano, ransomware), solo infectará la VM:

- no afectará al sistema real,
- no afectará a los archivos personales,
- no tendrá acceso a contraseñas almacenadas en el host.

La VM se convierte en una **zona de contención**, igual que un laboratorio aislado.

🔹 Beneficio 2: El router doméstico no ve el equipo real

Desde el punto de vista del router, el único sistema conectado a la red es la máquina virtual.
La máquina física (tu ordenador) permanece invisible.
Esto evita:

- fingerprinting del sistema real,
- ataques dirigidos al host,
- explotación de servicios abiertos,
- filtración de MAC real o identificadores sensibles.

🔹 Beneficio 3: Sesiones críticas más seguras

Acciones como:

- banca online,
- acceso a paneles IoT,
- administración del router,
- compras online,
- gestión de cuentas sensibles,

se pueden realizar desde una ISO recién montada, sin extensiones, sin historial y sin software malicioso residente.

Es como estrenar un sistema operativo cada vez que navegas.

🔹 Desventaja: rendimiento más lento

El profesor señala que esta técnica **no es la más cómoda**.
Una VM consume recursos y no es tan fluida como el sistema real, pero en términos de seguridad:

> es una de las soluciones más sólidas disponibles para usuarios domésticos sin hardware especializado.

📌 Conclusión del profesor sobre el aislamiento por VM

- Extremadamente seguro.
- Reduce enormemente el riesgo ante malware persistente.
- Ideal para actividades críticas.
- Especialmente útil cuando se administra una red IoT con dispositivos conectados.

El profesor refuerza la idea de que la ciberseguridad doméstica no solo consiste en contraseñas fuertes, sino en crear **barreras estructurales** que hagan más difícil que un atacante llegue al sistema principal del usuario.
